

# 2FA@NTU | Preparing for Two Factor Authentication (2FA) for the First Time for Student

Two Factor Authentication (2FA) provides an additional layer of security to protect against unauthorized access to NTU services and data. It requires two methods to verify your identity, which include (1) something you know i.e. your Office365 account username (i.e. username@e.ntu.edu.sg) and password, AND (2) something you have i.e. your mobile phone or the Microsoft Authenticator app configured on your mobile device to authenticate access. This guide provides **detailed step-by-step instructions on how you can complete the one-time enrolment process to activate 2FA.**

## 1 Install Microsoft Authenticator

a. You'll need both a computer and mobile device / smartphone to setup 2FA.



b. Download and install the **Microsoft Authenticator app** on your iOS or Android mobile device.



**NOTE:** Microsoft Authenticator app is supported on iOS 16.0 & above AND Android 9.0 & above (varies by devices).

## 2 Start the Enrolment

a. Login to [www.office.com](http://www.office.com) using your computer from the Internet



Please sign in using your Office365@NTU account credentials in the following format:

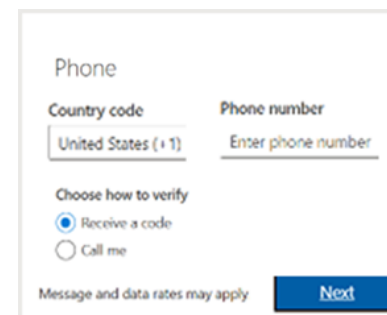
**username@e.ntu.edu.sg**

## 3 Configuring 2FA for Your Account

a. When you logon click on **Next** to start the 2FA enrolment



b. Enter your mobile phone number



- Select your **Country code** (where your mobile phone is registered)
- Your **Phone number**
- Choose **Receive a code** and click on **Next**

**Note: Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.**

c. You will receive a **6 digit verification code** on your registered phone

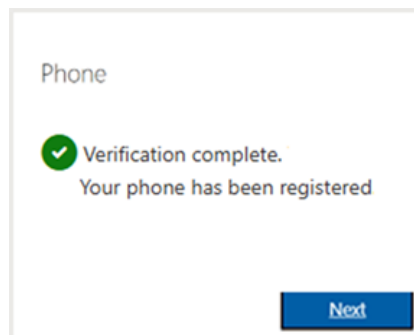


Enter this **6 digit code** in the dialog box

A screenshot of a Microsoft account verification dialog box titled 'Phone'. It says 'We just sent a 6 digit code' and has a text input field labeled 'Enter code'. Below the input field is a blue link that says 'Resend code'. At the bottom right is a blue button labeled 'Next'.

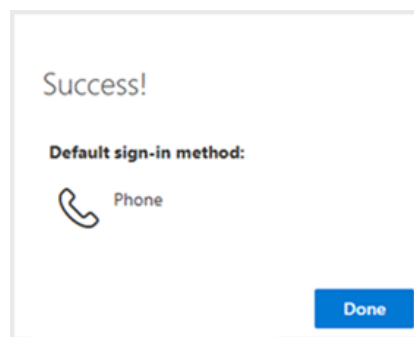
and then click **Next**

Once your mobile number had been registered successfully a **Verification complete** message will be displayed



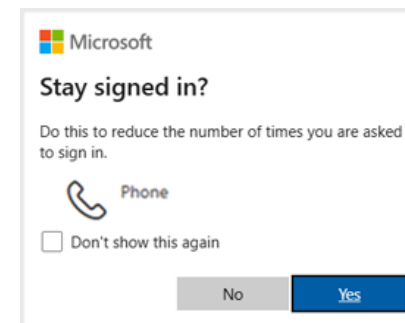
Click on **Next**

d. You'll then see a confirmation message your setup is completed as below



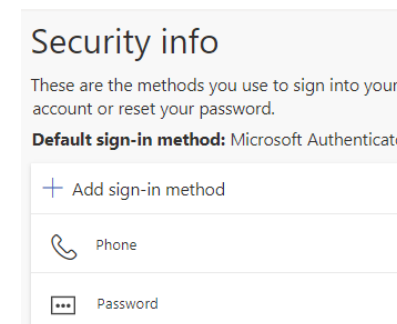
Click on **Done**

e. Click on **Yes** to continue the next part of the setup for **Self Service Password Reset**

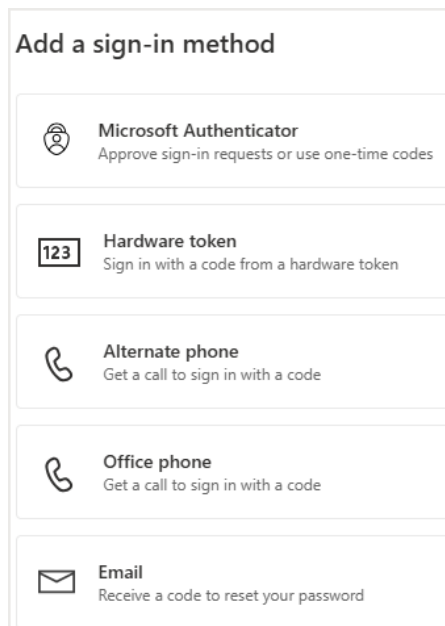


f. Go to this link <https://aka.ms/mfasetup>

Click on **+ Add sign-in method**



g. Click on  **Email** and follow the registration instructions on-screen to register your **external email address**



**Add a sign-in method**

-  **Microsoft Authenticator**  
Approve sign-in requests or use one-time codes
-  **Hardware token**  
Sign in with a code from a hardware token
-  **Alternate phone**  
Get a call to sign in with a code
-  **Office phone**  
Get a call to sign in with a code
-  **Email**  
Receive a code to reset your password

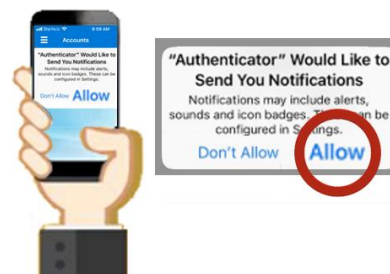
h. After registration of Email click on Click on **+** **Add sign-in method** again and select  **Microsoft Authenticator** and follow the registration instructions on-screen to setup Microsoft Authenticator on your mobile phone.

There will be a **QR Code** displayed on your computer that looks like this:

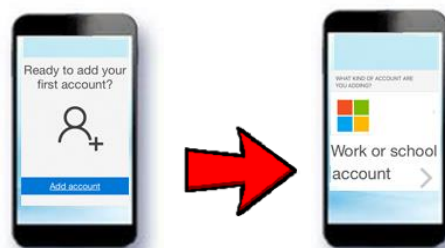


Launch the **Microsoft Authenticator** app on your mobile device and when prompted as shown below, select “**Allow**” notifications.

**NOTE:** Turn on notifications for the Microsoft Authenticator app so that you can receive notification on your phone when there is an access request.

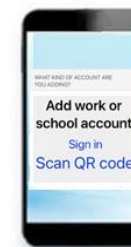


d. In the Microsoft Authenticator app, select “**Add account**” **+**



and choose “**Work or School account**”.

e. Select **Scan QR code**



Point your mobile device / smartphone camera to **scan the QR Code** on the web page.

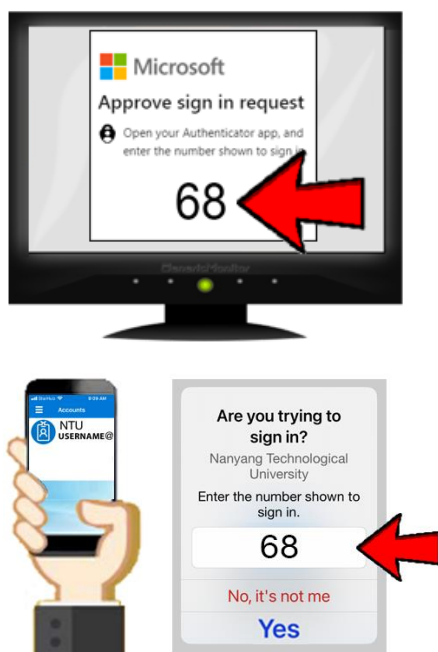
**NOTE:** Make sure you allow the Microsoft Authenticator app to access your phone camera.



Click on **Next**  on your computer.

You will then receive an access request on your mobile device / smartphone.

On your mobile device / smartphone, **enter** the **number** shown on your computer (in this example is “68”)

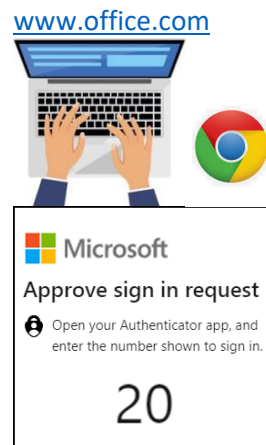


Click on “Yes” to complete the 2FA activation.

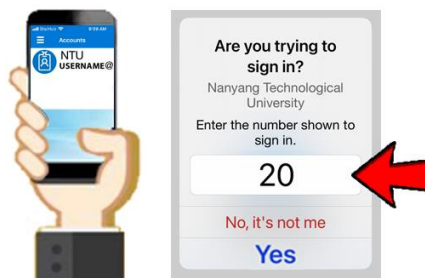
Your mobile device is now configured as a registered device for 2FA.

## 4 Signing In Using MS Authenticator

a. Login to [www.office.com](https://www.office.com) through a web browser.



b. On your mobile device / smartphone, **enter** the **number** shown on your computer (in this example is “20”) and click “Yes” to sign in.



**NOTE:** Microsoft caches user credentials for specific time duration. In most cases you will not be prompted to verify with 2FA for Office365 Apps (unlike web browsers) for **90 days** i.e. if you use the app on your mobile or computer more frequently than every 90 days.



Any changes that cause you to login again, such as a software update, will trigger 2FA verification. Things that could force you to re-authenticate:

- If you sign in and out of the Office clients again
- Not logged on for 14 days on that device
- Changed your password
- Software and App Updates after App restart
- Swapping between multiple Office 365 accounts

Administrators applying conditional policies to restricted resources you are trying to access